Release Notes for iPlanet™ Directory Access Router

Version 5.0

Updated July 23, 2001

These release notes contain important information about Version 5.0 release of iPlanet Directory Access Router (iDAR). New features and enhancements, installation notes, known problems, and other late-breaking issues are addressed here. Read this document before you begin installing and using iDAR.

These release notes contain the following sections:

- What's New in This Version

- iDAR Documentation

- Installation Notes

- Important Notes

- Known Problems and Limitations

- Resolved Bugs

- How to Report Problems

- For More Information

What's New in This Version

This release of iDAR includes the following changes (when compared to iDAR, version 2.1):

- The supported platforms list has changed; check the *iDAR Installation Guide* for details.

- Java based GUI consoles, called the *iDAR Server Console* and *iDAR Configuration Editor Console*, to aid in the configuration of iDAR. It's recommended that you use the iDAR consoles to configure and maintain new installations of iDAR.

- Several performance improvements and bug fixes; see section Resolved Bugs.

iDAR Documentation

The complete set of iDAR documentation for this release includes the following:

- **iPlanet Directory Access Router Release Notes** (this document)

  The release notes contain information on new features of this release, software/hardware requirements for installing the product, important notes and known bugs, last-minute product information, and how to send feedback.

- **iPlanet Directory Access Router Installation Guide**

  This document describes how to plan for and install iDAR. Read this document next, after you've read these release notes. Both HTML and PDF versions of this document are provided.

- **iPlanet Directory Access Router Administrator's Guide**

  This document provides detailed information on configuring and maintaining iDAR. Both HTML and PDF versions of this document are provided.

- **iPlanet Directory Access Router Frequently Asked Questions**

  This document contains answers to frequently asked questions, clarifications on iDAR features, and troubleshooting information. Both HTML and PDF versions of this document are provided. Note that the same document is included as an appendix in the *iDAR Administrator's Guide*.

After you run the `setup` script as described in the installation instructions, check this file for a list of documentation installed with the product: `<server-root>/manual/en/idar/index.htm`, where `<server-root>` is your iDAR installation directory. For the release notes, check this directory: `<server-root>/bin/idar`.

For the latest information about iDAR, including current release notes, technical notes, and deployment information, check this web site:
`http://docs.iplanet.com/docs/manuals/dar.html`

Installation Notes

Note the following:

- Software and hardware requirements and installation instructions are documented in the *iDAR Installation Guide*.

- If you have an existing installation of iDAR, before installing this version of iDAR, save any configuration files in the file system to a place outside of the iDAR install directory, and then uninstall the existing iDAR.

- After installing iDAR on a Windows NT system, make sure to reboot the system; you can do this from the Start menu.

Important Notes

This section contains important notes about the following:

- Migrating Configuration From iDAR 2.1 To iDAR 5.0

- Configuring iDAR For SSL/Certificates

- Generating Core Files

- Using the Support Tool

Migrating Configuration From iDAR 2.1 To iDAR 5.0

If you have an existing installation of iDAR 2.1, a tool has been provided to assist in the conversion of iDAR 2.1 configuration into one recognized by iDAR 5.0's console-based configuration. Using the configuration tool, you can import existing iDAR 2.1 configuration objects from an LDIF file into an instance of iPlanet Directory Server functioning as the *configuration directory*. This tool is useful for porting existing iDAR installations to this version of iDAR 5.0, which uses the iPlanet Console.

You can find the configuration tool in the following directory:

```
<server-root>/bin/idar/admin/script
```

Note that configuration objects are expected to appear in a known location in the directory (currently `ou=dar-config, o=netscaperoot`) and conform to a predefined structure. The tool is invoked as follows:

```
ImportConfigurationLdif <options> ldif
```

where, `ldif` is a required directive indicating where the tool is to find the LDIF file containing iDAR configuration objects and `options` can be substituted with the following:

`-C <configuration name>`

> The name of configuration to create/augment. Defaults to "imported-configuration".

`-h <host>`

> The hostname of the configuration directory. If omitted, the utility assumes "localhost".

`-p <port number>`

> The port number of the configuration directory. If omitted, the utility assumes 389.

`-D <bind dn>`

> The bind DN of the Directory user. If omitted, the utility will bind anonymously, but you may not be able to make updates.

`-w <password>`

> The password of the Directory user.

For example, the following command imports objects from the specified LDIF file, `sample.ldif`:

```
ImportConfigurationLdif -D uid=admin,ou=Administrators,ou=TopologyManagement,
o=netscaperoot -w admin sample.ldif
```

Configuring iDAR For SSL/Certificates

Chapter 5, "Configuring System Parameters" and Chapter 12, "Configuring Security" of the *iDAR Administrator's Guide* document how to set up iDAR for SSL-enabled communication. Here are a few additional notes that you should take into consideration when setting up iDAR for SSL-enabled communication:

• If iDAR is configured to verify client certificates (see Step 4 of "Steps to Configure TLS/SSL Support") the client cannot use SASL EXTERNAL to authenticate based on the subject DN of the client certificate. Instead, the client will have to use simple BIND, CRAM-MD5, or DIGEST-MD5, unless an anonymous BIND is sufficient.

- While it is possible to configure iDAR to present its certificate to a directory server, the clients of iDAR will still have to perform simple BINDs in order to present valid credentials over the SSL connection between iDAR and the directory server. The point is that simply validating iDAR to the directory server does not implicitly authenticate the iDAR client to the directory. iDAR does not use the proxy authentication control.

- When using certificates, make sure that the appropriate root certificates are known to the appropriate entities: to iDAR, to the directory servers, and to the LDAP clients. If any of these entities can't verify the root certificate path while validating a certificate, then it'll fail to communicate with the entity that presented the certificate.

  On iPlanet Directory Server (versions 4.11 and later), use the Certificate Setup Wizard, which can be launched from within the console, to import any necessary CA certificates. You might also have to make the appropriate changes to the `certmap.conf` file. For more information on setting up the Directory Server, check the Directory Server documentation at: `http://docs.iplanet.com/docs/manuals/directory.html`

  In iDAR, the file `<server-root>/idar-<hostname>/etc/rootcerts.pem` contains a list of root certificates in the PEM format. This list includes most of the common root CA certificates, but certificates such as "Thawte TEST CA" will have to be added as needed.

  Note that there can be up to three certificate paths involved, each with potentially different root certificates:

  ❍ The certificate list which iDAR presents to the LDAP client and to the directory server.

  ❍ The certificate list which the client presents to iDAR.

  ❍ The certificate list which the directory server presents to iDAR. iDAR 5.0 currently does not support having different certificate lists for communication to clients from that which it uses to authenticate to the directory server.

- If you configure iPlanet Directory Server (versions 4.11 or later) to require client authentication (this option is under the Encryption tab in the console), then you must also set the `ids-proxy-con-send-cert-as-client` attribute to TRUE in the iDAR configuration.

- iPlanet Directory Server 4.11 only supports RSA certificates. If you are going to configure Directory Server to require client authentication, you must ensure that the iDAR certificate has an RSA public key and an RSA signature. This consideration is relevant when using a DSA certificate for iDAR to be used with non-RSA clients over SSL or TLS.

Generating Core Files

On platforms other than Windows NT, iDAR cannot generate core files if the attribute `ids-proxy-con-userid` in the `ids-proxy-sch-GlobalConfiguration` object class is set to something other than the user that started the iDAR process. If you want iDAR to generate a core file in case it fails unexpectedly, set the above mentioned attribute to the same user that starts the iDAR process.

Using the Support Tool

A utility has been provided that allows you to retrieve iDAR's configuration from a directory and store it in a file in the LDIF format. This file can then be sent to product support for help with configuration problems or you can tell iDAR to use this file to configure itself on startup. (Check the *iDAR Administrator's Guide* for information related to the `tailor.txt` file.)

You can find the utility in the following directory:

`<server-root>/bin/idar/server/scripts/`

The utility takes the following options. Both options are required.

`-t <tailor filename>`

Where `<tailor filename>` is the path to the startup configuration file on disk.

`-o <output file>`

Where `<output file>` is the path of file where you want the configuration to be stored.

For example, the following command will read the `tailor.txt` file, retrieve the configuration from the location specified in the `tailor.txt` file, and save the configuration in the `tailor.ldif` file. (This example assumes the current working directory is an iDAR instance directory and the `iDARPrintConfig` command's location is in the environment's "PATH".)

`iDARPrintConfig -t tailor.txt -o tailor.ldif`

Note that the command does not actually print anything. It downloads the configuration for further consideration.

Known Problems and Limitations

This section lists known problems and provides workarounds for some of the problems that you may encounter with the product. Numbers enclosed within square brackets, for example, [548588], are bug numbers. Bug numbers are useful when discussing issues with Technical Support or Professional Services.

• Installation

• Miscellaneous

• UI (Console Interface)

• Uninstallation

Installation

• iDAR installation assumes that you are always installing iDAR on a server root that already has an instance of iPlanet Administration Server installed or you are installing it in conjunction with an Administration Server.

• Only one instance of iDAR can be installed on a given host. [548588]

• iDAR's console installation does not handle server root paths that possess "special" characters that are key word characters in TCL. For example, `[ ]` characters instruct TCL to perform a command. Thus, if the server root path possesses `[ ]` within it, it would cause certain parts of the installation to act improperly. The characters that should be avoided are as follows:

    ? " ' [ ] ( ) # . ~ $ ^ * +

• iPlanet Administration Server Console refuses to start if the `<server-root>` possesses an embedded space. Thus, it is recommended that you do not install using a `<server-root>` with an embedded space. [543176]

• iPlanet Administration Server that ships with iDAR cannot be installed on the same server root as an iWS 6.0 installation.

• The *iDAR Installation Guide* describes how to disable ports other than TCP 389 on Windows NT using the TCP/IP Properties on the Network Control Panel. Please be aware that disabling UDP may prevent DNS lookups from occurring properly. If your configuration makes use of domain names which iDAR must resolve using DNS, you should allow UDP as well as the TCP port for LDAP.

- On Windows, the installation routine isn't capable of sensing that the user has told iDAR to listen on the same port number as the iPlanet Administration Server. Thus, be sure to use a unique port to avoid complications. [541046]

- If you uninstall iDAR and plan to reinstall it on the same machine, make sure to follow either of the procedures listed below. Failure to do so may cause iDAR to fail to start or to not function properly. [548593]

  ○ Before installation, delete the configuration associated with the machine name on which you are installing iDAR. (You can delete the configuration either via the console or in the configuration directory itself.)

  ○ After installation, open the iDAR Server Console, go to the Configuration tab, enable the Save button by choosing configuration object <NONE>, select the configuration associated with the machine name, and click Save.

Miscellaneous

- iDAR supports a maximum of 32 back end directory servers across any single group.

- In case one of the back-end LDAP directory server hosts becomes unreachable from the host on which iDAR is running, clients that were virtually connected to that host may seem to hang as they wait for iDAR to time out its back-end connection. A fail over will be performed by iDAR when the connection gets timed out. The timeout is modifiable on Solaris systems. (Check the details about the `idsktune` utility. The utility gets installed at `<server-root>/shared/bin` and is explained in section "Operating System Requirements" of Chapter 2, "Computer System Requirements" in the *iDAR Installation Guide*.)

UI (Console Interface)

- The iDAR Configuration Editor Console fails to warn the user that a configuration reload is required (by recycling the server or by HUP) of all subscribing iDARs if a configuration object (Group, Action , Rule, Property, or System) is deleted.

- The iDAR Configuration Editor Console fails to warn the user that a configuration reload is required (by recycling the server or by HUP) of all subscribing iDARs if the user changes the priority of groups by using the Up/Down arrow buttons in the Group Object View.

- On Unix variants, the Console's "helper" functions used to determine if iDAR is up and running won't see iDAR if the `ldapfwd` iDAR is running is a symbolic link. This is only an issue if iDAR installation has been manually manipulated post installation. (In other words, don't rename iDAR's executable or convert it to a symbolic link.)

Uninstallation

- During uninstallation, iDAR does not remove all entries subordinate to `ou=dar-config, o=NetscapeRoot`. [548593]

- On Windows, the correct way to uninstall iDAR is to remove iDAR first and then subsequently uninstall the iPlanet Administration Server. [540694]

  The iDAR uninstallation must not be done simultaneously with the removal of its corresponding Administration Server. The reason for this is that when everything is being removed, the uninstall program stops the Administration Server and removes its service manager entry prior to iDAR's uninstall routines being given the opportunity to remove its configuration. Because iDAR depends on the Administration Server to carry out an uninstallation task, the Administration Sever should be up and functioning when iDAR is being uninstalled. If iDAR is uninstalled simultaneously with the Administration Server, it will leave its configuration subordinate to `ou=dar-config, o=NetscapeRoot` in the configuration repository untouched. This could cause undesired behavior with iDAR, should you reinstall iDAR on the same host and use the same configuration repository subsequently as it could see residual "belongs to" entries.

  Manual remedy should you not heed this advice: find all entries subordinate to `ou=dar-config, o=NetscapeRoot` whose `ids-proxy-sch-belongs-to` matches the host in question and remove the attribute. Note that the entry may be removed only if the entry no longer possesses any value for the `ids-proxy-sch-belongs-to` attribute.

Resolved Bugs

This section contains the list of bugs that have been resolved in this release of iDAR:

Table 1   List of Resolved Bugs

Bug Number	Description
440769	hopcount on referrals is not working
441849	TCL configuration tool and iDS ldif idiosyncrasies
441869	TCL configuration tool always decomposes DN
442009	TCL configuration tool doesn't handle quoted suffix
512817	`certreq` invoked with no option returns with file open errors
520001	StartTLS interoperability problem with iDS5.0

Table 1 List of Resolved Bugs *(Continued)*

Bug Number	Description
520002	Application error if directory server is not running
520063	Windows configuration tool only supports default install path
531360	Typos in configuration script error message
531361	LDIF file contains RDN values of parent entries
533854	Improve Logging in iDAR
534287	iDAR core dumps on referral following
534288	iDAR crash
540631	Security hole reported by CERT affects iDAR too
541798	NT files do not have access control restrictions
541891	CRTL-C kills ldapfw if started with /etc/rc.d/S93iDAR
542760	Support URL ldap:///
542807	Encoding error for large entries
543331	Crash on failover for server with 0 priority
546990	Reverse-DNS lookup fails in iDARv2.1, IP-addresses do work

How to Report Problems

If you have problems with iPlanet Directory Access Router, contact iPlanet customer support using one of the following mechanisms:

- iPlanet online support web site at
  http://www.iplanet.com/support/support_services_10_0.html

  From this location, the CaseTracker and CaseView tools are available for logging problems; these tools are available to customers with appropriate maintenance contracts.

- The telephone dispatch number associated with your maintenance contract

So that we can best assist you in resolving problems, please have the following information available when you contact support:

- Description of the problem, including the situation where the problem occurs and its impact on your operation

- Machine type, operating system version, and product version, including any patches and other software that might be affecting the problem

- Detailed steps on the methods you have used to reproduce the problem

- Any error logs or core dumps

You may also find it useful to subscribe to the following interest group, where iPlanet Directory Server topics are discussed:

```
snews://secnews.netscape.com/netscape.dev.directory
```

For More Information

Useful iPlanet information can be found at the following Internet locations:

- iPlanet release notes and other documentation — `http://docs.iplanet.com/docs/manuals/`

- iPlanet product status — `http://www.iplanet.com/support/technical_resources/`

- iPlanet Professional Services information — `http://www.iplanet.com/services/professional_services_3_3.html`

- iPlanet developer information — `http://developer.iplanet.com/`

- iPlanet learning solutions — `http://www.iplanet.com/learning/index.html`

- iPlanet product data sheets — `http://www.iplanet.com/products/product_map/product_name_2_0a.html`

For More Information